AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of

Information contained in and associated with the Google, Inc. email accounts antronrameygcinvestments@gmail.com, (Target Account #1) and grandcapitalus@gmail.com, (Target Account #2) and associated Google accounts

Case No. 1:19MJ4042 ACL

APPLICATION FOR A SEARCH WARRANT

I, Martin J. Williams, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A

located in the Northern District of California, there is now concealed

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, United States Code, Sections 1341 and 1343	Mail Fraud; Wire Fraud

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

☑ Continued on the attached sheet.

☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Martin J. Williams, S/A, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 3/12/2019

Judge's signature

City and state: Cape Girardeau, Missouri

Abbie Crites-Leoni, U.S. Magistrate Judge

Printed name and title

THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF MISSOURI SOUTHEASTERN DIVISION

IN THE MATTER OF THE SEARCH OF:
Gmail and Google accounts
Re Email user(s): antronrameygcinvestments@gmail.com (Target Account #1) and grandcapitalus@gmail.com (Target Account #2)

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Martin J. Williams ("Affiant"), a Special Agent (SA) with the Federal Bureau of Investigation (FBI) St. Louis Division, being duly sworn, depose and state as follows:

INTRODUCTION

I make this affidavit in support of an application for a search warrant for information associated with a certain electronic mail account that is stored, maintained, controlled, and/or operated by Google Inc. ("Google"), an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The accounts to be searched are antronrameygcinvestments@gmail.com (Target Account #1) and grandcapitalus@gmail.com, (Target Account #2), which are further described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C SS 2703(a), 2703(b)(1)(A) and 2703 (c)(1)(A), and Rule 41, Federal Rules of Criminal Procedure, requiring Google to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts referenced in this affidavit and further described in Attachment A, including contents of communications.

The FBI is investigating Antron F. Ramey for conducting a financial fraud scheme by means of wire and mail fraud in violation of 18 USC 1341 (Mail Fraud) and 18 USC

1343 (Wire Fraud). Throughout the investigation it has been determined the aforementioned Gmail e-mail accounts listed of Target Account #1 and Target Account #2 were being utilized to send and receive communications and attachments as those materials relate to this scheme. The use of Target Account #1 and Target Account #2 to further the fraudulent scheme is set out below in this affidavit.

AGENT BACKGROUND

1. I am a Special Agent (SA) with the FBI and have been so employed since March 1997. I am currently assigned to the St. Louis Division, Cape Girardeau Resident Agency of the FBI where I conduct a variety of criminal investigations. Since joining the FBI, I have been the case agent for numerous investigations of federal crimes related to mail fraud, wire fraud and financial fraud schemes. I have gained expertise in the conduct of such investigations through training, seminars, classes, and everyday work related to conducting these types of investigations.

2. The facts in this affidavit are based on my personal observations, my training, experience and information obtained from conducting interviews of numerous victims of Ramey's fraudulent scheme. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included every fact known to me concerning the investigation.

3. I have probable cause to believe evidence of violations of Title 18, United States Code, Sections 1341 and 1343, involving the use of a computer and the Internet, is located in and within the aforementioned accounts. I have probable cause to believe the accounts, that is the subject of this application, will have stored information and communications that are relevant to

this investigation, including evidence of the identity of the person maintaining the accounts and other email accounts associated with the email accounts, antronrameygcinvestments@gmail.com (Target Account #1) and grandcapitalus@gmail.com, (Target Account #2), and possible associated storage accounts. Based on my training and experience, there is probable cause to believe that evidence, fruits and/or instrumentalities of the aforementioned crimes are located in the accounts.

STAUTORY AUTHORITY

4. The investigation concerns the alleged violations of Title 18, United States Code, Sections 1341 and 1343, related to a financial fraud scheme. Based upon my training and experience, as well as conversations with other experienced law enforcement officers and federal prosecutors, the following statutes have been violated as set forth in this investigation:

a. 18 U.S.C. 1341: Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, or to sell, dispose of, loan, exchange, alter, give away, distribute, supply, or furnish or procure for unlawful use any counterfeit or spurious coin, obligation, security, or other article, or anything represented to be or intimated or held out to be such counterfeit or spurious article, for the purpose of executing such scheme or artifice or attempting so to do, places in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service, or deposits or causes to be deposited any matter or thing whatever to be sent or delivered by any private or commercial interstate carrier, or takes or receives therefrom, any such matter or thing, or knowingly causes to be delivered by mail or such carrier according to the direction thereon, or at the place at which it

is directed to be delivered by the person to whom it is addressed, any such matter or thing, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation occurs in relation to, or involving any benefit authorized, transported, transmitted, transferred, disbursed, or paid in connection with, a presidentially declared major disaster or emergency (as those terms are defined in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122)), or affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

b. 18 U.S.C. 1343: Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation occurs in relation to, or involving any benefit authorized, transported, transmitted, transferred, disbursed, or paid in connection with, a presidentially declared major disaster or emergency (as those terms are defined in section 102 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5122)), or affects a financial institution, such person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both.

5. The legal authority for this search warrant application is derived from Rule 41, Federal Rules of Criminal Procedure and Title 18, Untied States Code, Sections 2701 et seq., titled "Stored Wire and Electronic Communications and Transactional Records Access."

6. Title 18, United States Code, Section 2703(c)(A) allows for nationwide service of process of search warrants for the contents of electronic communications. Pursuant to 18 U.S.C. 2703(b) & (b), as amended by the USA PATRIOT Act, Section 220, a government entity may require a provider of an electronic communication service or a remote computing service to disclose a record or other information pertaining to a subscriber or customer of such service pursuant to a warrant issued using procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation.

INFORMATION REGARDING GOOGLE

7. Based upon my training, as well as conversations with other law enforcement officers, I have learned that Google offers a variety of online services, including email access and file hosting services, to the general public. Google allows subscribers to obtain email accounts at the domain name "gmail.com" like the emails listed in Attachment A. Subscribers obtain an account by registering online with Google. During the registration process Google requests subscribers to provide basic information, such as name, gender, zip code and other personal / biographical information. However, Google does not verify the information provided. Therefore, the corporate servers of Google are likely to contain stored electronic communications (including retrieved and un-retrieved email messages) and information concerning subscribers and their use of Google's services, such as account access information, email transaction information, and account application information.

8. I have learned that an email sent to a Google "gmail.com" subscriber, is stored in the subscriber's "Inbox" on Google servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on the Google servers

indefinitely. The user can move and store messages in personal folders such as a "sent" folder. Based on my training and conversations with other law enforcement officers with experience in executing search warrants of email accounts, I know that search warrants for email accounts and computer media may reveal stored emails sent and / or received long prior to the date of the search.

9. Based on my training and experience, as well as conversations with other experienced law enforcement officers, I know that when the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination. Google often saves a copy of the email sent.

10. I know that a sent or received email typically includes the content of the message, source and destination address, the date and time at which the email was sent, and the size and length of the email. If an email user writes a draft message but does not send it, that message may also be saved by Google but may not include all of these categories of data.

11. Based on my training and experience, as well as conversations with other experience law enforcement officers, I know a Google subscriber can also store files, including emails, address books, contact or buddy lists, calendar data, pictures, videos and other files on servers maintained and / or owned by Google. Subscribers to a Google account might not store on their home computers copies of the emails or images stored in their Google account. This is particularly true when they access their Google account through the Internet and/or via a smartphone, or if they do not wish to maintain particular email of files in their residence.

12. I know individuals often use email accounts for everyday transactions because it is in fact, low-cost, and simple to use. People use email to communicate with friends and family,

manage accounts, pay bills, and conduct other online business. Email users often keep records of these transactions in their email accounts, to include indentifying information such as name and address.

13. Based on my training and experience, I know that evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and other files.

14. I know a user can access files stored on a Google account, including images and videos, from any device with an Internet connection as long as the proper account credentials, which are the user name and password, are provided. Google accounts can be access from devices such as computers, tablets and cellular telephones.

BACKGROUND OF THE INVESTIGATION

15. On September 19, 2019 The Federal Bureau of Investigation, St. Louis Division opened an investigation based on information indicating Antron F. Ramey is fraudulently soliciting investors to purchase various securities, without proper license. This scheme is being perpetrated utilizing electronic communications and the United States Postal Service. Ramey is keeping the proceeds fraudulently collected from victims.

16. On or around August 31, 2018 contact was initiated with Aislinn Andrews, Staff Attorney, Arkansas Securities Commission. Andrews provided information indicating the Arkansas Securities Commission is conducting an investigation of Ramey, for violations of offering and/or selling securities through the use of fraud, misstatements and omitted information. On March 28, 2018 the Arkansas Securities Commission issued a Cease and Desist

of Antron F. Ramey and AFR Brokerage LLC. AFR Brokerage is a company established by Ramey.

17. On September 6, 2018 Casey Stuart, Jackson, Missouri advised of investing money with Ramey without receiving a return on her investment and losing the original invested funds. Stuart was introduced to Ramey by Jerricah Whitmore, Chaffee, Missouri. Whitmore had previously invested approximately $1,300 with Ramey and appeared to be making significant returns on her investment. Based on information provided by Whitmore, contact was established with Ramey by Stuart.

18. Ramey told Stuart that Ramey was a financial investment advisor working on behalf of Grand Capital. Grand Capital is a legitimate investment company, with investors from many countries. Based on my communications with representatives of Grand Capital, Antron F. Ramey is not employed by, working with, or associated with Grand Capital in any manner. Ramey presented and had Stuart sign a Financial Services Agreement. Stuart stated the Financial Services Agreement, along with other related documents, were sent to her via email address antronrameygcinvestments@gmail.com, (Target Account #1). The agreement, dated August 8, 2018, states Jesse Stuart and Casey Stuart entered into a contract agreement with Grand Capital. Grand Capital will provide services related to the following markets: Foreign Exchange Market, known as Forex, Cryptocurrency and or Binary Options.

19. On September 6, 2018 Stuart provided a check to Ramey, made payable to Grand Capital. The check was in the amount of $1,000. The check's payable to line was later altered adding the name Antron R after Grand Capital. Ramey subsequently deposited the check into his personal Bank of America account via a mobile banking application. After becoming skeptical

of Ramey, Stuart contacted Grand Capital who advised Ramey was not an employee of Grand Capital.

20. On September 6, 2018 contact was made by this agent with Jerricah Whitmore. Whitmore advised investing $1,300 with Ramey. Whitmore stated that Ramey provided her information indicating her investment had grown significantly in a short period of time. Whitmore eventually received a check from Ramey in the amount of $19,000, The check was dated September 1, 2018 and drawn on the account of Grand Capital at Western Alliance Bank, Phoenix, Arizona. The memo section of the check indicated the purpose was Investment Withdrawal. Whitmore deposited the check into her account at the Bank of Advance, Advance, Missouri. The check was subsequently returned as being fictitious, meaning that the check was not authorized to be written on that account.

21. Subsequent contact with Western Alliance Bank confirmed the check as being fictitious. The account number, listed on the check, belongs to Prime Trust, Las Vegas, Nevada. Further the account was closed in August 2018.

22. The $19,000 Grand Capital check was sent to Whitmore via the United States Postal Service (USPS). The USPS envelope indicated the package was sent on August 22, 2018 with an expected delivery of August 25, 2018. The package displayed a return address of being sent from Scott Purcell, 2300 W. Sahara Ave, Suite 1170, Las Vegas, Nevada 89102. The package had a USPS Signature Tracking Number of 9510 8116 2702 8234 1855 20.

23. On September 12, 2018 contact was made with George Georgiades, General Counsel, Prime Trust, 2300 W. Sahara Ave, Suite 1170, Las Vegas, Nevada. Georgiades stated

Scott Purcell is the Chief Executive Office and Chief Trust Officer of Prime Trust. Neither Purcell nor Prime Trust are affiliated with Grand Capital.

24. On September 24, 2018 contact was made with Matthew Murrow, United States Postal Inspector, Springfield, Missouri. Murrow was asked to provide assistance on identifying where the package was sent from via the USPS Signature Tracking Number 9510 8116 2702 8234 1855 20. Murrow indicated the USPS Package was mailed from Batesville, Arkansas on August 22, 2018 at 4:31 p.m. I have discovered that the residential address for Antron F. Ramey is 274 Dry Run Circle, Batesville, Arkansas.

25. On November 7, 2018 contact was made with Crystal Rodgers, Fuquay Varina, North Carolina. Rodgers advised being a victim of a financial fraud scheme perpetrated by Ramey. Rodgers was introduced to Ramey by Dylan Dannenmueller, Oran, Missouri. Dannenmueller indicated he was investing funds with Ramey and gaining excellent returns on his investments, based on reports he was receiving from Ramey. Based on the information from Dannenmueller, Rodgers agreed to meet with Ramey.

26. On April 24, 2018 Rodgers met Ramey at the Broussard's Restaurant in Cape Girardeau, Missouri. Also present during the meeting was Whitmore. Ramey represented himself as being the owner of AFR Brokerage. Ramey explained AFR Brokerage invested funds in the crypto-currency markets utilizing a company called Grand Capital. Rodgers advised signing an AFR Brokerage contract with Ramey.

27. Rodgers gave Ramey $3,000 in U.S. currency. Ramey provided Rodgers an AFR Brokerage LLC invoice dated April 24, 2018. The AFR invoice indicates on April 24, 2018 AFR received $3,000 from Rodgers.

28. Rodgers advised receiving a Grand Capital check in the amount of $19,200 dated August 20, 2018 and drawn on Western Alliance Bank, Phoenix, Arizona. This check was to represent funds withdrawn from Rodger's Grand Capital account after she was told her investment had increased to approximately $24,000. Rodgers asked Ramey to withdrawal $16,200 plus her initial $3,000 investment. The Grand Capital check was sent via U.S. mail.

29. Rodgers deposited the check into her Wells Fargo checking account. Shortly thereafter Wells Fargo contacted Rodgers to advise the check was fictitious. Since being advised the check was fictitious Rodgers has been unable to obtain any funds from Ramey.

30. Subsequent contact with Western Alliance Bank confirmed the check as being fictitious. The account number listed on the check belongs to Prime Trust, Las Vegas, Nevada. Further the account was closed in August 2018.

31. On November 9, 2018 Robert J. Grojean, Chaffee, Missouri, was interviewed regarding his knowledge of Ramey. Grojean indicated investing $1,600 with Ramey believing Ramey to be an investment broker.

32. Grojean was introduced to Ramey through Adam Schaefer. Schaefer advised of investing funds with Ramey and making a significant return on the investment. After hearing of Schaefer's successful investments Grojean obtained Ramey's phone number.

33. Grojean advised talking with Ramey about investing funds with Grand Capital. Grojean believed Ramey to be associated with Grand Capital in some manner. Grojean agreed to invest funds with Ramey after hearing of the potential return on the

investment. Ramey subsequently emailed a Financial Services Agreement to Robertj@reagan.com from email account antronrameygcinvestments.com (Target Account #1).

34. On June 12, 2018 Grojean and James Wasson, a co-worker of Grojean, met with Ramey at Grojean's residence. During this meeting Ramey opened a Grand Capital account for both Grojean and Wasson. This was done via the internet using a computer located at Grojean's residence. During this meeting Grojean signed the Financial Service Agreement previously emailed from Ramey.

35. Grojean wrote a check for $1,600 made payable to Ramey, with the understanding the funds would be invested in Grojean's Grand Capital account. Ramey advised the investment should return approximately $300,000 in five years. This information was reflected in the Financial Services Agreement.

36. Grojean last talked with Ramey on or around September 2018. During the conversation Ramey advised Grojean's investment balance was approximately $5,300. Grojean has attempted to contact Ramey since but has been unsuccessful.

37. On November 9, 2018 James Wasson, Scott City, Missouri, was interviewed in Chaffee, Missouri. Wasson advised becoming familiar with Ramey through Schaefer. Schaefer is a friend of Wasson. Schaefer had indicated Ramey was an investment broker. Ramey had invested money for Schaefer and the investment was making excellent returns.

38. On June 12, 2018 Ramey met with Wasson and Grojean at Grojean's residence located in Chaffee, Missouri. Prior to the meeting Ramey emailed a Financial Services

Agreement to Wasson's email address groceryman81@live.com. Ramey sent the document via email address antronrameygcinvestments@gmail.com, (Target Account #1).

39. Wasson provided Ramey a check in the amount of $1,000. The check were funds to be invested by Ramey and deposited in a Grand Capital investment account. Since investing the funds Wasson has been unable to gain access to the Grand Capital account set up by Ramey. Wasson believes Ramey failed to deposit the funds with Grand Capital and kept the money for himself. Wasson has attempted to make contact with Ramey but has been unsuccessful.

40. On November 26, 2018 Debbie Erives-Palacious (Erives-Palacious), Olathe, Colorado was interviewed. Erives-Palacious became familiar with Ramey through Selene Berumen. Berumen is a friend who had invested funds with Ramey. The investment appeared to be increasing per reports Berumen was obtaining from Ramey, via text messages.

41. After several discussions regarding Berumen's investments, Berumen provided Ramey's telephone number and Facebook profile to Erives-Palacious. In June 2018 Erives-Palacious made contact with Ramey to inquire about investment opportunities. Ramey indicated being an investment broker, utilizing Grand Capital to facilitate trades.

42. On June 4, 2018 Ramey emailed Erives-Palacious a Financial Services Agreement which allowed Ramey to invest funds on behalf of Erives-Palacious. The contract was sent to Erives-Palacious email account debbieyivan@gmail.com from Ramey's email account antronrameygcinvestments@gmail.com, (Target Account #1). On June 6, 2018 Erives-Palacious signed the agreement and emailed it to Ramey.

43. Erives-Palacious indicated to Ramey, she was needing to make $40,000 to assist in paying back a loan provided by relatives. Ramey advised if she would invest between $5,000 to $10,000, a $40,000 return would be possible within two months. This goal was reflected on the Financial Services Agreement.

44. On June 11, 2018 Ramey sent an email providing bank wire details for his bank account at First Midwest Bank, Dexter, Missouri. The instructions were sent from antronrameygcinvestments@gmail.com, (Target Account #1). The email indicates Ramey is a National Account Manager for Grand Capital.

45. Erives-Palacious attempted to wire $5,000 to Ramey's First Midwest Bank of Dexter, Missouri bank account. The wire was returned due to a bank security issue. After not receiving the funds, Ramey contacted Erives-Palacious to advise he was conducting trades, on her behalf, believing the funds were being transferred. Ramey needed the funds to offset the investments he had made for Erives-Palacious.

46. On June 13, 2018 Erives-Palacious sent $5,000 to Ramey utilizing a wire transfer from her Wells Fargo bank account. Ramey advised receiving the funds the same day.

47. Erives-Palacious advised of receiving a check from Ramey on August 25, 2018. The check was dated September 1, 2018, in the amount of $45,000, and drawn on the account of Grand Capital at Western Alliance Bank. The funds were to represent a withdrawal from her Grand Capital investment account. The check was sent utilizing an USPS envelope containing USPS Signature Tracking Number 9510 8116 2702 8234 1855 37. The envelope identified the sender as Scott Purcell, 2300 W. Sahara Ave, Suite 1170, Las Vegas, Nevada

89102 and the recipient as Debbie Palacious, 6225 David Rd., Olathe, Colorado 81425. Erives-Palacious advised of not depositing the check. Erives-Palacious talked with Berumen who stated receiving a check from Grand Capital as well. When Berumen deposited the check it came back as fictitious. Berumen's checking account was subsequently closed by the bank. Erives-Palacious did not want this to happen with her account as she believed the check was fictitious.

48. A review of the check sent to Erives-Palacious reveals the same account number as previous fictitious checks Ramey sent to other victims. Contact with Western Alliance Bank confirmed the checking account number listed on the check belongs to Prime Trust, Las Vegas, Nevada. Further the account was closed in August 2018.

49. On November 27, 2018 contact was again made by this agent with Matthew Murrow, United States Postal Inspector. Murrow was asked to identify where the USPS envelope, bearing USPS Signature Tracking Number 9510 8116 2702 8234 1855 37, originated. This package was referenced in the preceding paragraph. Murrow provided information indicating the USPS envelope was mailed from Batesville, Arkansas on August 22, 2018 at 4:33 p.m. Batesville, Arkansas is the city where Ramey keeps his primary residence.

50. Erives-Palacious indicated receiving emails from what she believed to be Grand Capital via email account grandcapitalus@gmail.com, (Target Account 2). The emails advised of daily and weekly returns on her Grand Capital account. On August 28, 2018 Erives-Palacious sent an email to Grand Capital Support inquiring on her account. The email was sent to clients@grandcapital.net.

51. On August 29, 2018 Erives-Palacious received information from Grand Capital Client Support, clients@grandcapital.net, indicating she was a victim of a scam. The email advised all Grand Capital emails end with @grandcapital.net and Erives-Palacious' Grand Capital account had never been credited with any funds. Grand Capital further indicated Ramey is not an employee of Grand Capital and they do not have offices in Las Vegas, Nevada.

52. Erives-Palacious received information from Ramey indicating he was wiring her $25,000 from her Grand Capital account. Erives-Palacious received an email confirmation of the wire from what was made to appear it was being sent from Bank of America. The email was sent from antonrameygcinvestments@gmail.com, (Target Account #1). Erives-Palacious explained knowing the transaction was fraudulent as she previously provided Ramey fictitious wire transfer instructions. Erives-Palacious provided Ramey a closed bank account number and a routing number that had one extra numeral. This was done in effort to see if he would confirm the transaction had been sent, which he did by sending the email indicating the wire was successfully transferred.

53. Erives-Palacious' last conversation with Ramey was on September 11, 2018. During the conversation Ramey indicated he was wiring her the balance in her Grand Capital account. Erives-Palacious has not received any funds from Ramey.

54. On November 27, 2018 contact was made by this agent with Alejandra Erives, Montrose, Colorado. Erives and her husband, Samuel Erives, were introduced to Ramey through Debbie Erives-Palacious. Erives-Palacious is Erives' sister-in-law. Erives-Palacious provided Erives the Facebook profile for Ramey.

55. Erives contacted Ramey via Facebook messenger. After the initial contact Ramey provided telephone number (870) 613-8243 for additional contact.

56. Ramey stated that he was a National Account Manager for Grand Capital, an investment company. Erives was unfamiliar with Grand Capital. After discussing investment opportunities and the possible investment returns, Ramey sent Erives a Financial Services Agreement. The Financial Services Agreement was sent on June 27, 2018 from email account antronrameygcinvestments@gmail.com, (Target Account #1). The document was sent to Erives' email account calejandra56@yahoo.com. Prior to signing the Financial Services Agreement, Erives discussed how much money was needed to invest. Ramey indicated $500 was the minimum investment accepted. Erives indicated having $7,000 to invest. Ramey stated the $7,000 would return $45,000 within two months. This information was listed on the Financial Services Agreement. On June 27, 2018 Samuel Erives signed the Financial Services Agreement and emailed it to antronrameygcinvestments@gmail.com, (Target Account #1).

57. Ramey provided Erives information as to where the $7,000 investment should be wired. Upon receiving the instructions funds were wired to Ramey's First Midwest Bank account, Dexter, Missouri. The funds were sent in two different wire transactions. The first wire was sent on June 29, 2018 in the amount of 5,000. The second wire was sent on July 2, 2018 in the amount of $2,000.

58. Erives advised of receiving Grand Capital investment financial updates via text messages from Ramey's cell phone. The text messages indicated the current values of the investment account. On one occasion, Ramey sent Erives a text message indicating her investment had exceeded the original goal of $45,000.

59. Erives obtained information indicating Ramey was running a financial fraud scheme and had stolen money from Crystal Rodgers and others. Upon obtaining this information, Erives' husband contacted a Grand Capital customer support representative. Information was provided indicating Erives' Grand Capital account had never received a deposit.

60. On December 6, 2018 Selene Berumen, Coachella, California, was interviewed by this agent. Berumen advised being married to Eric Vasquez. Both Berumen and Vasquez are victims of a financial fraud scheme perpetrated by Ramey. Berumen advised learning of Ramey through Crystal Rodgers. Rodgers advised of making significant returns on money she invested with Ramey. Rodgers provided Berumen's contact information to Ramey.

61. On May 22, 2018 Ramey contacted Berumen via Facebook messenger. On May 23, 2018 Berumen and Vasquez invested $500 with Ramey. Funds were sent from Berumen's Wells Fargo account to Ramey. Ramey was to invest the funds on behalf of Berumen. Shortly afterwards Ramey provided instructions on how to set up a Grand Capital investment account utilizing the Grand Capital mobile application.

62. Berumen recalled Ramey emailing a Financial Services Agreement from email address antronrameygcinvestments@gmail.com, (Target Account #1). The email was sent to selene.berumen@yahoo.com. The Financial Services Agreement was signed and sent back to antronrameygcinvestments@gmail.com, (Target Account #1).

63. Believing her account was making tremendous profits, on or about June 28, 2018 Berumen wired an additional $2,000 to Ramey from her Wells Fargo account. In addition, on July 13, 2018 Vasquez wired $2,000 to Ramey.

64. On August 13, 2018 Berumen received a $36,000 Grand Capital check based on a withdrawal request made to Ramey. The check was dated August 25, 2018 and drawn on the account of Grand Capital, 2300 W. Sahara Ave, Suite 1170, Las Vegas, Nevada at Western Alliance Bank, Phoenix, Arizona. The checks was sent via the USPS. The USPS envelope indicates the check was sent from Scott Purcell, 2300 W. Sahara Ave, Suite 1170, Las Vegas, Nevada. Berumen advised depositing the check into her personal checking account at Wells Fargo Bank. The check was subsequently deemed fictitious causing an insufficient funds status with her bank. Berumen contacted Ramey who indicated the checks were issued erroneously by Grand Capital.

65. Subsequent contact with Western Alliance Bank confirmed the check as being fictitious. The account number, listed on the check, belongs to Prime Trust, Las Vegas, Nevada. Further the account was closed in August 2018.

66. Berumen tried to obtain the balance of her Grand Capital account on numerous occasions but was unable to verify a balance. Berumen made contact with Ramey who indicated the Grand Capital website was down. Ramey subsequently provided her updated balances via text message. Berumen has yet to receive any money from Ramey.

67. Berumen advised referring Rocio Berumen and Elliew Silva Hernandez to Ramey. Rocio invested $7,000 and Hernandez invested $2,000 with Ramey. Both wired funds to Ramey's bank account in Missouri. Neither person obtained any funds from Ramey. Due to

Rocio and Hernandez speaking limited English, Berumen facilitated the communication between Rocio, Hernandez and Ramey.

PROCEDURES FOR ELECTRONICALLY STORED INFORMATION

68. Federal agents and investigative support personnel are trained and experienced in identifying communications relevant to the crimes under investigation. The personnel of Google are not. It would be inappropriate and impractical for federal agents to search the vast computer network of Google for the relevant accounts and then to analyze the contents of those accounts on the premises of Google. The impact on Google's business would be severe.

69. Therefore, I request the authority to seize all content, including electronic mail and attachments, from the Google email and cloud accounts described in Attachment A. In order to accomplish the objective of the search warrant and with a minimum of interference with the business activities of Google, to protect the rights of the subject of the investigation and to effectively pursue this investigation, authority is sought to allow Google to make a digital copy of the entire contents of the accounts subject t o seizure. The copy will then be forensically analyzed to identify communications and other data subject to seizure.

70. Analyzing the data to be provided by Google may require special technical skills, equipment and software. It also can be very time consuming. Searching by keywords, for example, often yields many thousands of "hits," each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Certain file formats do not lend themselves to keyword searches. Keywords search text. Many common electronic mail database and spreadsheet applications, which files may have been attached to electronic mail, do not store data

as searchable text. The data is saved in a proprietary non text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases dramatically.

71. Based on the foregoing, searching the recovered data for information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or months. Keywords need to be modified continuously based upon the results obtained.

72. Based upon my experience, training and the experience of other law enforcement officers I have had conversations with, it is necessary to review and seize all electronic mails that identify any users of the subject accounts and any electronic mails sent or received in temporal proximity to incriminating emails that provide context to the incriminating emails. All forensic analysis of the data will be directed exclusively to the identification and extraction of data within the scope of this warrant.

REQUEST TO SEAL, ORDER NON-DISCLOSURE, & KEEP ACCOUNT ACTIVE

73. Because the investigation is ongoing, I request this Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested search and seizure warrants, including applications, this affidavit, and the requested warrants. I believe that sealing these documents are necessary because the items and information to be seized are relevant to an ongoing investigation. It is likely that if the contents of this affidavit are made public, that evidence of the fraudulent wire and bank transfers referenced above may be destroyed. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

74. Pursuant to Title 18, United States Code, Section 2705(b), I would request the Court order Google not to disclose the existence or service of the search and seizure warrants to the subscriber, customer, or any other person until otherwise ordered by the court, except as required to disclose to Google officers, employees, or agents to the extent necessary to comply with the warrant. The basis for this motion is that providing notification at this time of the warrant may result in the destruction of or tampering with evidence and have a significant and negative impact on the investigation.

75. Because the investigation is ongoing, I would further request the Court to order Google to continue to maintain the email accounts antronrameygcinvestments@gmail.com, (Target Account #1) and grandcapitalus@gmail.com, (Target Account #2) along with any additional related Google email and/or storage accounts in an open and active status.

CONCLUSION

76. Based on my training, experience, and the facts as set forth above, I have probable cause to believe that on the computer systems in control of the Google, there exists evidence of crime(s), contraband and / or fruits of a crime(s). Specifically, I have probable cause to believe the email accounts antronrameygcinvestments@gmail.com, (Target Account #1) and grandcapitalus@gmail.com, (Target Account #2), contains evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1341 and 1343. Accordingly, a search warrant is requested.

77. Pursuant to Title 18, United States Code, Section 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Martin J. Williams
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 12th day of March, 2019, in Cape Girardeau, Missouri.

Abbie Crites-Leoni
Honorable Abbie Crites-Leoni
U.S. MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

This warrant applies to information contained in and associated with the Google, Inc email accounts antronrameygcinvestments@gmail.com, (Target Account #1) and grandcapitalus@gmail.com, (Target Account #2), associated Google accounts, which are stored at the premises owned, maintained, controlled or operated by Google, Inc., 1600 Amphitheatre Parkway, Mountain View, California 94043 and other locations where data relating to requested accounts may be stored.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED

I Information to be disclosed by Google, Inc..

To the extent that the information for the accounts described in Attachment A is within the possession, custody, or control of Google, Inc., Google, Inc. is required to disclose the following information to the government for the accounts listed in Attachment A. Such information should include the following:

1. The contents of the email account antronrameygcinvestments@gmail.com, (Target Account #1) and grandcapitalus@gmail.com, (Target Account #2), to include copies of all emails sent to and from the account, the source and destination addresses associated with each email message, the date and time at which each email message was sent, and the size and length of each email message.

2. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number).

II Information to be seized by the government

All information described above in Section I, including messages and attachments that constitute fruits, evidence and instrumentalities of the violations of Title 18, United States Code,

Sections 1341 and 1343 and also including for the accounts listed in Attachment A, the following items:

1. Credit card and other financial information, including but not limited to, bills and payment records, evidencing ownership of the accounts listed in Attachment A.

2. Evidence of who used, owned, or controlled the accounts listed in Attachment A.

3. Evidence of the times that the accounts listed in Attachment A was used.

4. Passwords and encryption keys, and other access information that may be necessary to access the account or identifier listed in Attachment A and other associated Accounts.

III By Order of the Court

1. The Court orders Google, Inc. not to notify any person of the existence of this warrant.

2. The Court further orders Google, Inc. to continue to maintain the email account and cloud storage account listed in Attachment A in an open and active status, so as not to disrupt this ongoing investigation.